

Docket No. P13066

Serial No. 10/037,239

**IN THE CLAIMS:**

Please amend claims 1, 8, 19, 29, 36, 43, and 54, as set forth below.

1           1.       (Currently Amended) A computer implemented method comprising:  
2 reading distinguished name data from a signed certificate received from a certificate  
3 authority, the signed certificate received in response to a certificate signing  
4 request provided to the certificate authority, the certificate signing request  
5 validating an identity to the certificate authority; and  
6 searching a data structure to identify [[a]] the certificate signing request associated with  
7 the signed certificate, the identified certificate signing request corresponding to  
8 the read distinguished name data.

1           2.       (Original) The method of claim 1, further comprising identifying a key  
2 pair associated with the signed certificate.

1           3.       (Original) The method of claim 1, the read distinguished name data  
2 comprising all of the distinguished name data contained in the signed certificate.

1           4.       (Original) The method of claim 1, the identified certificate signing request  
2 corresponding to a portion of the read distinguished name data.

1           5.       (Original) The method of claim 1, further comprising importing the  
2 signed certificate to a server associated with the identified certificate signing request.

1

Docket No. P13066

Serial No. 10/037,239

1

1           6.       (Original) The method of claim 5, wherein the signed certificate is  
2 imported to a device that performs SSL processing on behalf of the server.

1

1           7.       (Original) The method of claim 1, further comprising identifying at least  
2 two certificate signing requests associated with the signed certificate.

1

1           8.       (Currently Amended) A computer implemented method comprising:  
2 providing a mapping table including distinguished name data for each of a plurality of  
3 certificate signing requests, each certificate signing request validating an identity;  
4 extracting distinguished name data from a signed certificate received from a certificate  
5 authority; and  
6 comparing the extracted distinguished name data with the mapping table data to identify  
7 a certificate signing request associated with the signed certificate from the  
8 plurality of certificate signing requests.

1

1           9.       (Original) The method of claim 8, the mapping table including at least a  
2 common name for each of the plurality of certificate signing requests.

1

1           10.      (Original) The method of claim 8, the extracted distinguished name data  
2 comprising all of the distinguished name data contained in the signed certificate.

1

Docket No. P13066

Serial No. 10/037,239

1

1 11. (Original) The method of claim 8, the extracted distinguished name data  
2 comprising a common name.

1

1 12. (Original) The method of claim 8, further comprising comparing a portion  
2 of the extracted distinguished name data with a portion of the distinguished name data of  
3 each certificate signing request contained in the mapping table to identify the certificate  
4 signing request associated with the signed certificate.

1

1 13. (Original) The method of claim 12, the portion of the extracted  
2 distinguished name data comprising a common name.

1

1 14. (Original) The method of claim 8, further comprising:  
2 comparing the extracted distinguished name data with the mapping table data to identify  
3 at least two certificate signing requests from the plurality of certificate signing  
4 requests; and  
5 determining which of the at least two certificate signing requests is associated with the  
6 signed certificate.

1

1 15. (Original) The method of claim 14, further comprising performing a  
2 second search of the mapping table data to determine which of the at least two certificate  
3 signing requests is associated with the signed certificate.

1

Docket No. P13066

Serial No. 10/037,239

1

1 16. (Original) The method of claim 8, further comprising importing the  
2 signed certificate to a server associated with the identified certificate signing request.

1

1 17. (Original) The method of claim 16, wherein the signed certificate is  
2 imported to a device that performs SSL processing on behalf of the server.

1

1 18. (Original) The method of claim 8, further comprising identifying at least  
2 two certificate signing requests associated with the signed certificate.

1

1 19. (Currently Amended) A computer implemented method comprising:  
2 generating a certificate signing request, the certificate signing request including  
3 distinguished name data;  
4 storing the distinguished name data in a mapping table;  
5 transmitting the certificate signing request to a certificate authority, the certificate signing  
6 request validating an identity to the certificate authority;  
7 receiving a signed certificate from the certificate authority, the signed certificate  
8 including distinguished name data;  
9 extracting the distinguished name data from the signed certificate; and  
10 comparing the extracted distinguished name data with the stored distinguished name data  
11 contained in the mapping table to identify the certificate signing request.

1

Docket No. P13066

Serial No. 10/037,239

1

1           20.     (Original) The method of claim 19, the stored distinguished name data  
2 comprising all of the distinguished name data contained in the certificate signing request.

1

1           21.     (Original) The method of claim 19, the stored distinguished name data  
2 comprising a common name.

1

1           22.     (Original) The method of claim 19, further comprising comparing a  
2 portion of the extracted distinguished name data with a portion of the stored distinguished  
3 name data.

1

1           23.     (Original) The method of claim 19, further comprising comparing a  
2 common name contained in the extracted distinguished name data with a common name  
3 contained in the stored distinguished name data.

1

1           24.     (Original) The method of claim 19, the extracted distinguished name data  
2 comprising all of the distinguished name data contained in the signed certificate.

1

Docket No. P13066

Serial No. 10/037,239

1

1           25.   (Original) The method of claim 19, the extracted distinguished name data  
2 comprising a common name.

1

1           26.   (Original) The method of claim 19, further comprising:  
2 generating a key pair associated with the certificate signing request; and  
3 identifying the key pair when comparing the extracted distinguished name data with the  
4 stored distinguished name data.

1

1           27.   (Original) The method of claim 19, further comprising importing the  
2 signed certificate to a server associated with the certificate signing request.

1

1           28.   (Original) The method of claim 19, further comprising importing the  
2 signed certificate to an SSL processing device.

1

Docket No. P13066

Serial No. 10/037,239

1

1           29.     (Currently Amended) A computer system comprising:  
2     a memory coupled with a bus, the memory having a mapping table resident thereon; and  
3     a processing device coupled with the bus, the processing device programmed to perform  
4         operations including  
5             reading distinguished name data from a signed certificate received from a  
6             certificate authority, the signed certificate received in response to a  
7             certificate signing request provided to the certificate authority, the  
8             certificate signing request validating an identity to the certificate  
9             authority, and  
10            searching the mapping table to identify [[a]] the certificate signing request  
11            associated with the signed certificate, the identified certificate  
12            signing request corresponding to the read distinguished name data.

1

1           30.     (Previously Presented) The computer system of claim 29, wherein the  
2     processing device is programmed to perform operations further including identifying a  
3     key pair associated with the signed certificate.

1

1           31.     (Previously Presented) The computer system of claim 29, the read  
2     distinguished name data comprising all of the distinguished name data contained in the  
3     signed certificate.

1

Docket No. P13066

Serial No. 10/037,239

1

1 32. (Previously Presented) The computer system of claim 29, the identified  
2 certificate signing request corresponding to a portion of the read distinguished name data.

1

1 33. (Previously Presented) The computer system of claim 29, the memory  
2 comprising a non-volatile data storage device.

1

1 34. (Previously Presented) The computer system of claim 29, wherein a  
2 plurality of servers are coupled with the bus, and the processing device is programmed to  
3 perform operations further including downloading the signed certificate to a selected  
4 server of the plurality of servers, the selected server associated with the identified  
5 certificate signing request.

1 35. (Previously Presented) The computer system of claim 29, wherein an SSL  
2 processing device is coupled with the bus, and the processing device is programmed to  
3 perform operations further including downloading the signed certificate to the SSL  
4 processing device.

Docket No. P13066

Serial No. 10/037,239

1           36.   (Currently Amended) An article of manufacture comprising:  
2   a computer readable medium providing content that, when accessed by a computer,  
3   causes the computer to  
4       read distinguished name data from a signed certificate received from a certificate  
5       authority, the signed certificate received in response to a certificate  
6       signing request provided to the certificate authority, the certificate signing  
7       request validating an identity to the certificate authority; and  
8       search a data structure to identify [[a]] the certificate signing request associated  
9       with the signed certificate, the identified certificate signing request  
10      corresponding to the read distinguished name data.

1           37.   (Previously Presented) The article of manufacture of claim 36, wherein  
2   the content, when accessed, further causes the computer to identify a key pair associated  
3   with the signed certificate.

1           38.   (Original) The article of manufacture of claim 36, the read distinguished  
2   name data comprising all of the distinguished name data contained in the signed  
3   certificate.

Docket No. P13066

Serial No. 10/037,239

1           39.   (Original) The article of manufacture of claim 36, the identified certificate  
2 signing request corresponding to a portion of the read distinguished name data.

1           40.   (Previously Presented) The article of manufacture of claim 36, wherein  
2 the content, when accessed, further causes the computer to import the signed certificate to  
3 a server associated with the identified certificate signing request.

1

1           41.   (Previously Presented) The article of manufacture of claim 40, wherein  
2 the content, when accessed, further causes the computer to import the signed certificate to  
3 a device that performs SSL processing on behalf of the server.

1

1           42.   (Previously Presented) The article of manufacture of claim 36, wherein  
2 the content, when accessed, further causes the computer to identify at least two certificate  
3 signing requests associated with the signed certificate.

1

Docket No. P13066

Serial No. 10/037,239

1

1

43. (Currently Amended) An article of manufacture comprising:

2

a computer readable medium providing content that, when accessed by a computer,

3

causes the computer to

4

provide a mapping table including distinguished name data for each of a plurality

5

of certificate signing requests, each certificate signing request validating

6

an identity;

7

extract distinguished name data from a signed certificate received from a

8

certificate authority; and

9

compare the extracted distinguished name data with the mapping table data to

10

identify a certificate signing request associated with the signed certificate

11

from the plurality of certificate signing requests.

1

1

44. (Original) The article of manufacture of claim 43, the mapping table

2

including at least a common name for each of the plurality of certificate signing requests.

1

1

45. (Original) The article of manufacture of claim 43, the extracted

2

distinguished name data comprising all of the distinguished name data contained in the

3

signed certificate.

1

1

46. (Original) The article of manufacture of claim 43, the extracted

2

distinguished name data comprising a common name.

1

Docket No. P13066

Serial No. 10/037,239

1

1           47.   (Previously Presented) The article of manufacture of claim 43, wherein  
2   the content, when accessed, further causes the computer to compare a portion of the  
3   extracted distinguished name data with a portion of the distinguished name data of each  
4   certificate signing request contained in the mapping table to identify the certificate  
5   signing request associated with the signed certificate.

1

1           48.   (Original) The article of manufacture of claim 47, the portion of the  
2   extracted distinguished name data comprising a common name.

1

1           49.   (Previously Presented) The article of manufacture of claim 43, wherein  
2   the content, when accessed, further causes the computer to:  
3   compare the extracted distinguished name data with the mapping table data to identify at  
4   least two certificate signing requests from the plurality of certificate signing  
5   requests; and  
6   determine which of the at least two certificate signing requests is associated with the  
7   signed certificate.

1

Docket No. P13066

Serial No. 10/037,239

1

1 50. (Previously Presented) The article of manufacture of claim 49, wherein  
2 the content, when accessed, further causes the computer to perform a second search of the  
3 mapping table data to determine which of the at least two certificate signing requests is  
4 associated with the signed certificate.

1

1 51. (Previously Presented) The article of manufacture of claim 43, wherein  
2 the content, when accessed, further causes the computer to import the signed certificate to  
3 a server associated with the identified certificate signing request.

1

1 52. (Previously Presented) The article of manufacture of claim 51, wherein  
2 the content, when accessed, further causes the computer to import the signed certificate to  
3 a device that performs SSL processing on behalf of the server.

1

1 53. (Previously Presented) The method of claim 43, wherein the content,  
2 when accessed, further causes the computer to identify at least two certificate signing  
3 requests associated with the signed certificate.

1

Docket No. P13066

Serial No. 10/037,239

1

1

54. (Currently Amended) An article of manufacture comprising:

2

a computer readable medium providing content that, when accessed by a computer,

3

causes the computer to

4

generate a certificate signing request, the certificate signing request including

5

distinguished name data;

6

store the distinguished name data in a mapping table;

7

transmit the certificate signing request to a certificate authority, the certificate

8

signing request validating an identity to the certificate authority;

9

receive a signed certificate from the certificate authority, the signed certificate

10

including distinguished name data;

11

extract the distinguished name data from the signed certificate; and

12

compare the extracted distinguished name data with the stored distinguished name

13

data contained in the mapping table to identify the certificate signing

14

request.

1

1

55. (Original) The article of manufacture of claim 54, the stored distinguished

2

name data comprising all of the distinguished name data contained in the certificate

3

signing request.

1

Docket No. P13066

Serial No. 10/037,239

1

1 56. (Original) The article of manufacture of claim 54, the stored distinguished  
2 name data comprising a common name.

1

1 57. (Previously Presented) The article of manufacture of claim 54, wherein  
2 the content, when accessed, further causes the computer to compare a portion of the  
3 extracted distinguished name data with a portion of the stored distinguished name data.

1

1 58. (Previously Presented) The article of manufacture of claim 54, wherein  
2 the content, when accessed, further causes the computer to compare a common name  
3 contained in the extracted distinguished name data with a common name contained in the  
4 stored distinguished name data.

1

1 59. (Original) The article of manufacture of claim 54, the extracted  
2 distinguished name data comprising all of the distinguished name data contained in the  
3 signed certificate.

1

1 60. (Original) The article of manufacture of claim 54, the extracted  
2 distinguished name data comprising a common name.

1

Docket No. P13066

Serial No. 10/037,239

1

1           61.   (Previously Presented) The article of manufacture of claim 54, wherein  
2 the content, when accessed, further causes the computer to:  
3 generate a key pair associated with the certificate signing request; and  
4 identify the key pair when comparing the extracted distinguished name data with the  
5 stored distinguished name data.

1

1           62.   (Previously Presented) The article of manufacture of claim 54, wherein  
2 the content, when accessed, further causes the computer to import the signed certificate to  
3 a server associated with the certificate signing request.

1

1           63.   (Previously Presented) The article of manufacture of claim 54, wherein  
2 the content, when accessed, further causes the computer to import the signed certificate to  
3 an SSL processing device.